IPC wrapper

ddaa

Inter-Process Communication

- 不同 process 之間傳送資訊
- child 執行 service，parent 攔截 i/o

nc secprog.cs.nctu.edu.tw 10001

input filter: flag、/bin/sh、….
output filter: flag pattern、fake flag、…

execute service

Pipe wrapper

```
26      pipe(p1);
27      pipe(p2);
28      pid = fork();
29
30      if (!pid){ //parent
31          signal(SIGALRM, timeout);
32          alarm(10);
33
34          close(p1[0]);
35          close(p2[1]);
36
37          // get
38          n = read(p2[0], buf, BUFSIZE);
39          write(1, buf, n);
40
41          while (1) {
42              // hijack input
43              n = read(0, buf, BUFSIZE);
44              if (strstr(buf, "flag")) { // filter
45                  fprintf(stderr, "pwn?\n");
46                  exit(0);
47              }
```

Pipe wrapper

```
57      } else { //child
58          close(p1[1]);
59          close(p2[0]);
60          dup2(p1[0], 0);
61          dup2(p2[1], 1);
62          chdir("/home/applestore");
63          execve("./applestore", NULL, NULL);
64          exit(0);
65      }
```

Socket wrapper

```
29      unlink(SOCK_PATH);
30      int s = socket(AF_UNIX, SOCK_STREAM, 0);
31      struct sockaddr_un addr;
32      memcpy(addr.sun_path, SOCK_PATH, strlen(SOCK_PATH));
33      addr.sun_family = AF_UNIX;
34      bind(s, (struct sockaddr *)&addr, strlen(addr.sun_path) + sizeof(addr.sun_family));
35      listen(s, 5);
```

```
73          int s = socket(AF_UNIX, SOCK_STREAM, 0);
74          struct sockaddr_un addr;
75          bzero(addr.sun_path, sizeof(addr.sun_path));
76          memcpy(addr.sun_path, SOCK_PATH, strlen(SOCK_PATH));
77          addr.sun_family = AF_UNIX;
78          connect(s, (struct sockaddr *)&addr, strlen(addr.sun_path) + sizeof(addr.sun_family));
79          dup2(s, 0);
80          dup2(s, 1);
81          execve("./applestore", NULL, NULL);
82          exit(0);
```

Tips

- 注意程式原本是用哪個 function 做 io，用相同的方式與 client 對接比較不會出錯
- 在不做 filter 的情況下，wrapper 不能防止 attacker 拿走 flag
- 注意特殊字元（\n、\r、\x00……等等），是不是也可完整的送到 child
- 用 strace 來 debug 觀察 wrapper 行為是否正常

Notice

- 盡可能符合 service 原始行為，才能通過service check
- 也可以試著以 debugger、emulator 作為 wrapper
  - 但是 service check 不一定會通過……，主辦方可能也不會允許
  - 可能會有副作用，像是 NX 被關掉之類的 XD
- 如果 wrapper 沒寫好，SLA 可能就先扣一堆分了……
- 找到漏洞 && patch 才是最穩妥的方式